

Page Denied

Next 1 Page(s) In Document Denied

~~SECRET~~


DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-325

24 September 1982

MEMORANDUM FOR: Members, DCI Security Committee

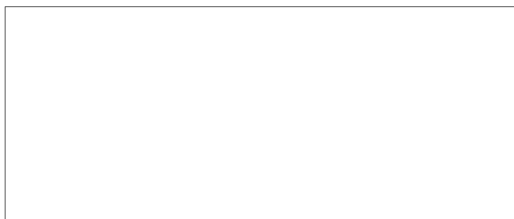
25X1 FROM:


Chairman

SUBJECT: Security Committee Seminar - IV

REFERENCE: SECOM-D-322, Dated 21 September 1982

Referenced memorandum circulated agenda topics suggested for the Security Committee Seminar. One of those topics was the NSA member's proposal on leaks. Attached for your information is a copy of his proposal.



~~SECRET~~



**NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE**
FORT GEORGE G. MEADE, MARYLAND 20755

Serial: M5/0058/82

16 July 1982

MEMORANDUM FOR THE CHAIRMAN, DCI SECURITY COMMITTEE

SUBJECT: Unauthorized Disclosures

1. The recent spate of serious intelligence disclosures in the news media serves to illustrate the need to studiously review our traditional response to such occurrences. Although "leaks" investigations may serve some useful purpose in deterrence, and they therefore should be continued, they have not been successful in preventing them. Furthermore, it appears that the sources of many of the disclosures are senior officials who are not fully aware of the sensitivity of our intelligence product.

2. I therefore propose that the Security Committee consider establishing a cadre of individuals whose task would be to conduct specialized briefings of senior government officials emphasizing the need to protect intelligence sources and methods. A program would be developed for these individuals to brief newly appointed government officials and to conduct regular follow-on briefings. Additionally, members of this group, although not empowered to authorize the public release of Sensitive Compartmented Information, could provide instantaneous individualized guidance on proposed public statements and direct officials to the proper agency for indepth questions and declassification authority. Although security officers experienced in briefing and awareness functions should be included in this group, obviously operational and/or information security officers should also be included. Extension of this proposed service to lower level officials, particularly those with press contact, should also be considered.

3. I am reminded that the Security Committee was originally established to address the problem of unauthorized disclosures. Although I am well aware of recent efforts by the Unauthorized Disclosures Investigations Subcommittee, we must vigorously pursue alternative attempts to alleviate the problem. I believe the time has come for the Security Committee and, indeed, the Intelligence Community, to make a substantial commitment in addressing this problem. Resources should be identified for the establishment of this specialized group, and it should be supported in such a way as to receive a high degree of visibility. Furthermore, the Director of Central Intelligence should be asked to seek a Presidential directive specifying that no government official be permitted to receive SCI without having been duly briefed about the perishable quality of intelligence product.

Declassify and mark
FOR OFFICIAL USE ONLY
upon removal of
enclosure.

HANDLE VIA COMINT CHANNELS ONLY

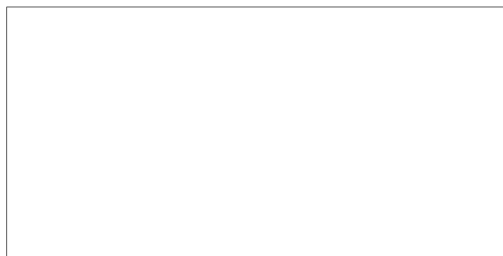
SECRET

Serial: M5/0058/82

4. As a second initiative in this area, we have prepared the attached draft letter for ultimate delivery to each Signals Intelligence user by his SOIC. This action is responsive to the NFIB position taken at their 8 June 1982 meeting following deliberations relative to the recent intelligence disclosures.

5. Because of the pressing nature of the unauthorized disclosures problem, I would have liked discussion of my proposal during the Security Committee meeting on 21 July 1982. However, as this is not possible, perhaps a special meeting could be called to consider my proposal.

Encl:
a/s



STAT

PL 86-36

SECRET

Serial:

MEMORANDUM FOR THE NATIONAL FOREIGN INTELLIGENCE BOARD MEMBERS

SUBJECT: Security Advisory to Recipients of United States Signals Intelligence (U)

(U) In furtherance of the NFIB decision of 8 June, the following letter has been drafted for Senior Officials of the Intelligence Community (SOIC's) to provide to SIGINT recipients. Each organization may modify the letter as appropriate; the principal point is the expression of concern about recent disclosures, and the reaffirmation of the sensitivity and fragility of Signals Intelligence sources and methods.

"(S-CCO) You are being provided this letter by reason of your access to, and actual receipt of, classified Signals Intelligence (SIGINT) produced by the National Security Agency (NSA) through its interception and decipherment of communications of foreign intelligence interest. You may receive such SIGINT either directly from NSA or in intelligence dissemination by other agencies. Every recipient of this letter has been cleared for access to TOP SECRET CODEWORD information; every recipient receives highly classified foreign intelligence, including SIGINT; the United States has placed the highest confidence and trust possible in every recipient. I regret to have to advise you that some recipients appear to have violated this trust by improperly disclosing to persons in the news media information revealing current, successful United States SIGINT activities, including, in one instance, an actual, deciphered message text.

"(S-CCO) It is important that all users understand the fragility of SIGINT, the ease with which countermeasures can be devised, and the serious consequences which can follow from such disclosures, even inadvertent or well-intentioned disclosures which may seem innocuous. Neither the text of messages nor the fact of decryption need to be disclosed in order to endanger NSA's abilities; virtually any release of SIGINT-derived or related information, including even sanitized disclosures, permits foreign states to draw conclusions concerning our targets, capabilities and techniques. We are aware from SIGINT that the recent unauthorized disclosures have been so analyzed by foreign nations. Without going into detail, my conclusion is that the leaks have endangered the United States SIGINT system, a priceless national resource, and have raised fundamental questions about our continued ability to collect and disseminate SIGINT.

"(U) While the security of SIGINT is protected by various statutes, (18 U.S.C. §793 and 798 among them) the utility of other measures, including administrative sanctions, should not be ignored. The basic protection for SIGINT, however, must be the prudence and legality of those persons provided access. The purpose of this letter is to remind you of these facts.

HANDLE VIA COMINT CHANNELS ONLY

SECRET

SC-06743-82

Cy 1

Serial:

"(U) I am taking this extreme measure in order to stress the unprecedented seriousness of my concern. I request that each recipient of this memorandum ensure distribution to all individuals within their respective organizations who receive signals intelligence, in any form, with the added requirement that such individuals acknowledge by signature their understanding of the concerns expressed herein."

(Organization SOIC)

(Signature of SIGINT Recipient)"

SC-06743-82